Correctness of the Fisher Yate Shuffle

Author: syscl/Yating Zhou

November 21, 2018

The code is attached in the same repository as **code.cc**. And we have to prove the correctness of the algorithm.

Theorem The probability of each element in each position from the returned array is the same.

Proof. For the base case, if the returned array has size 1, the probability of 1 stays in 1 is 1, and if the returned array has size 2, the probability of 1 stays in 1 is when we do not swap 1 and 2, so that is $\frac{1}{2}$, and the probability of 1 stays in the second position is thus $\frac{1}{2}$. For the inductive steps, suppose the probability of each element in each position of an array with size k is $\frac{1}{k}$, then for a given element to stay in a position $1 \leq i \leq k$ is thus when we do not swap this element at the i-th position (i.e., we swap elements other than i-th element), that is the probability of $\frac{1}{k}(1-\frac{1}{k+1}) = \frac{1}{k+1}$, if $i = k+1$, then the probability is $\frac{1}{k+1}$ because it is only when we swap the latest $k+1$-th element with the given element, so for a given element to stay in $1 \leq i \leq k+1$ position, the probability is thus $\frac{1}{k+1}$, which completes the proof. $\square$

Note, we can prove/explain the algorithm in another aspect. For a k distinctive elements ordered set, there is A_k^k possible combination of the sets and for a given element α be fixed in one position, we can generate A_{k-1}^{k-1} sets, that is for a given element α in a fixed position from 1 to k, the probability is $\frac{A_{k-1}^{k-1}}{A_k^k}$, and for the $k+1$ rounds of the routine, the α to stay in the original position is thus we swap elements other than α, that is

$$\frac{A_{k-1}^{k-1}}{A_k^k}(1 - \frac{1}{k+1}) = \frac{(k-1)!}{k!}\frac{k}{k+1} = \frac{1}{k+1} \tag{1}$$

(1) is what we want.